



**Homeland Security Advisory Council  
HSAS Task Force  
Stakeholder Feedback**

**Table of Contents:**

**Summary Memo of Stakeholder Feedback .....3**  
Theme 1: The color-codes/ maintaining a common vocabulary .....3  
Theme 2: Specificity .....3  
Theme 3: The levels .....4  
Theme 4: The system’s audience .....4  
Theme 5: Credibility and cost .....4

**Federal Government Agencies Responses to Homeland Security Advisory System Review**

**Questions .....6**  
**Synthesized Interagency Input about the HSAS ..... 12**  
**Additional Comments from the Interagency: ..... 14**  
**Response from Professor Philip Zimbardo ..... 16**  
**Synthesized Public Communications Stakeholder Summary ..... 19**  
**Synthesized DHS S&T Comments from Randy Beardsworth ..... 26**  
Human Systems Integration Notes: .....26  
START document notes\*: .....27  
Community Resilience Summary Notes\*: .....27

**Suggestion from HSAC Member, Kareem Shora ..... 29**  
Current drawbacks: .....29  
Constructive suggestions: .....29  
Conclusion: .....29

**Synthesized Private Sector Comments ..... 30**  
General .....30  
Colors and Categories .....30  
The Dynamics of Level Changes and Supplemental Information Provision .....31  
System Uses and Tie-ins .....31

**A Unified Emergency Scale from a Practitioner’s View: ..... 34**  
**A Public Warning System and Practitioner Notification System ..... 34**  
**Response by Dr. Sutton of Natural Hazards Center ..... 41**  
**First Responder Stakeholder Outreach Summary Findings Report ..... 46**  
**Pennsylvania Emergency Management Agency Suggestions ..... 51**

**ATTACHMENT I: Dr. Breckinridge Feedback**  
**ATTACHMENT II: CT HSAS Response**  
**ATTACHMENT III: Multi-State ISAC 2006**  
**ATTACHMENT IV: Unified Scale Academic Report**

# Summary Memo of Stakeholder Feedback

## Information

MEMORANDUM FOR: Homeland Security Advisory System Task Force

FROM: Office of Policy Development

SUBJECT: Stakeholder Feedback

This memo is in response to your request for a summary of stakeholder feedback about the Homeland Security Advisory System (HSAS).

**Stakeholder Outreach:** The Policy HSAS Review Support Group solicited comments from the following stakeholder groups:

- State, local, and tribal governments and community groups
- Federal agencies
- Private sector
- First responders
- Communications thought leaders (academics in the field of communications and others working in media)
- The public at-large (via [hsasreview@dhs.gov](mailto:hsasreview@dhs.gov), set up by Office of Public Affairs)

**Summary of Stakeholder Feedback:** Several themes about the current HSAS emerged following review of stakeholder feedback. These themes are: the importance of a common vocabulary; concerns regarding lack of specificity of the current warnings and unclear criteria for changing threat levels; and considering the intended audience for the alert system.

### ***Theme 1: The color-codes/ maintaining a common vocabulary***

While there was acknowledgement of problems with how the current notification system was implemented, several stakeholders noted one beneficial aspect of a graduated color-coded methodology. Namely, the color's ability to serve as "a common reference tool" or an "easy single point of reference" was amongst the positive attributes of HSAS that many stakeholder groups noted. This common sentiment demonstrated the need for any revised HSAS to utilize some sort of common vocabulary, even if that goal is not facilitated through use of a graduated color based system.

### ***Theme 2: Specificity***

The most common theme amongst stakeholder comments was the need for increased specificity as to the nature of any terrorist threat. Stakeholders almost universally commented that specific information on geographic location and industry is crucial for an alert system to be effective. Many comments emphasized that greater specificity is needed to facilitate an appropriate local response. In addition, several stakeholders voiced frustration with past warnings that they considered to be too vague to be useful. They pointed out that lack of details directed at a specific region or sector demonstrated that a nationwide threat alert was not only unnecessary, but also counterproductive

and/or costly for members not affected by the warning. One group even called the HSAS warnings “useless” because it does not provide enough information about geographic region or the nature of the threat.

Relatedly, some commenters argued that any new system should make recommendations on how local groups should organize for and respond to threats. Another group recommended that warnings contain details on what measures the federal government is taking in response to a particular threat. Others called for a more autonomous local response, with the federal government only providing minimal advice. Several commenters pointed to ready.gov as a starting point for informing the public on protective measures that they should take in response to a change in threat level.

### ***Theme 3: The levels***

Related to specificity are comments about the nature of the threat levels themselves. Specifically, stakeholders commented on the need for a clearer explanation of what criteria are associated with raising the terror alert level. Several groups called for a more specific definition of what constitutes a particular threat level, or at least explanation or justification for any change to the threat level so as to reduce the appearance of arbitrariness or perceived political manipulation. Other groups called for a so called sunset or “expiration” for a terror alert, with the level automatically going back to a status-quo unless the federal government explained why it must remain elevated.

Suggestions for a simpler graduated system also included an all-hazards/all threats system, or even using the Department of Defense’s DEFCON system as a model. Several stakeholders called for a reduction of the number of colors from five to three, while noting that the lowest two levels have not been used since HSAS’s inception.

### ***Theme 4: The system’s audience***

Stakeholders also made comments on the desired audience for the alert system. Some emphasized the need for media and the public to be closely involved in any alert system. In contrast, others downplayed the public’s ability to take specific actions in response to any terrorist threats and questioned the necessity of telling the public too many details. The thrust of these comments is that a revised system should focus on government officials charged with responding to threats, rather than focusing on the public at large. No one called for shutting out the public entirely, but one group did note the difficulty of providing public information without disclosing potentially sensitive intelligence.

### ***Theme 5: Credibility and cost***

Many stakeholders indicated that the HSAS is ineffective because it lacks credibility. Different groups emphasized the need to rebuild trust in the system through transparency and increased specificity. Commenters noted that use of the media, “new media” (generally meaning internet communications), and public education may be part of restoring this trust to any advisory system. Regardless, it is clear that the stakeholder groups recognized the need to engage in outreach with both the public and local authorities in order to ensure system credibility.

In addition, several stakeholders noted the monetary and public effects of changing threat level alerts. Some groups mentioned the cost to law enforcement for maintaining a high threat level. In

terms of public anxiety stemming from the alert changes, suggested public education initiatives and better explanations of threats can mitigate public panic and anxiety.

# Federal Government Agencies Responses to Homeland Security Advisory System Review Questions<sup>1</sup>

Note: The questions below are intended as a flexible guide to assist in framing HSAS Task Force discussions and should be tailored to the experience and expertise of individual respondents.

1. Is the Homeland Security Advisory System (HSAS) effective in fulfilling its purposes as stated in 6 U.S.C. § 124 and HSPD-3, namely: (I) does it provide to Federal, State, local and tribal authorities and to the people of the United States, as appropriate, advisories or warnings regarding the threat or risk that acts of terrorism will be committed on the homeland; (II) does it provide, in each such advisory or warning, specific information and advice regarding appropriate measures and countermeasures that may be taken in response to the threat or risk, at the maximum level of detail practicable to enable individuals, government entities, emergency response providers, and the private sector to act appropriately; and (III) does it create common vocabulary, context, and structure for discussion about threats and appropriate courses of action?

DoD → (I) No: HSAS does not provide advisories and warnings regarding the threat or risk that attacks of terrorism will be committed in the homeland. To substantiate this point, since its creation in 2002 the HSAS color has varied only between the levels of yellow and red. That means, during a period when the United States has experienced only a few intermittent clear and present threats (such as the summer of 2006), we have failed to distinguish substantially between those periods and periods of lesser threat. Everyone understands that there is a constant and unpredictable threat of terrorism, just as there was a constant threat of nuclear annihilation during the Cold War. But the HSAS should do better to distinguish between the “general threat” (which should correspond to color code “blue”) and periods when the U.S. government has uncovered actual credible threat streams (which should correspond to other color codes depending on the level of information we have obtained about the credibility of the threat).

(II) No: HSAS does not mandate any DoD posture changes as there is no direct correlation between HSAS and DoD’s Force Protection Condition system.

(III) No: DoD is unaware of any influence that HSAS exerts over “vocabulary, context, and structure for discussion about threats and courses of action.”

---

<sup>1</sup> The listed answers were compiled from responses to Key Study Questions about the Homeland Security Advisory System (HSAS). All wording is original from the responsible agency, with only some formatting changes to fit this page and for clarity. All grammar and syntax is original to the authoring agency.

a. **What are the system's strengths with respect to these purposes?**

DoD→ In DoD's opinion, the system has no readily identifiable strengths in any of these three areas.

USDA→The current system is simple and easy to understand. It provides a common vocabulary and a general sense of the level of threat without providing specific information as to the threat itself.

GSA→The strength of the system is that it provides a uniformed readiness baseline for all government agencies to employee measures to detect, deter, mitigate, and respond to potential threats.

b. **What are the system's weaknesses with respect to these purposes?**

DoD→ See above. Because HSAS does not tie changes in the color code to significant U.S. government prevention activities, it is a weak system that generates more public anxiety than public awareness.

USDA→

- The preponderance of personnel who actively respond to changes in the system are law enforcement and facility physical security staffs. The system does not generate a widespread response from the public.
- The five-tiered system loses credibility when "normal" operating status is in the middle of the chart.
- People have become enured to the current system since the threat level seldom changes.
- The current system does not provide information on appropriate and reasonable measures or countermeasures. It also does not provide information on the specific sector or geographic area threatened.
- Current system is focused on terrorism, however, the recommended actions in the *Citizen Guidance on the Homeland Security Advisory System* are appropriate for all-hazards, including natural disasters.
- The current system is not addressed in the planning process. Federal plans developed under the Integrated Planning System do not address actions taken in response to changes in HSAS threat advisory levels.
- Many times events are responded to without a change in the HSAS
- Current HSAS is not coordinated with COGCON/COOP/MARSEC. Should it be?

GSA→One of the weaknesses associated with the system is that it does not specifically identify measures designed to progressively harden federal assets based upon the increased likelihood of a terrorist attack based upon the specified advisory level.

2. **What changes, if any, would improve the current system?**

DoD→ Increasing the HSAS level should drive immediate changes in U.S. government activities, much like changes in DoD's various conditions. DEFCON, FPCON, et cetera all have associated

activities as the condition level increases and decreases. This keeps DoD from being able to keep the condition levels high for no reason, since increasing the condition levels commensurately increases response optempo and, frankly, creates additional costs that cannot be permanently sustained.

An additional potential consideration for the HSAS is the implementation of two systems: AGENCY (Federal, State and Local) (confidential) and PUBLIC (unclassified). The AGENCY system would be a compulsory system for federal agencies similar to the DOD FPCON model. It would provide detailed guidance for state and local officials based upon a specific threat.

USDA→

**a. Is the purpose in HSPD-3, as stated, the right purpose regarding:**

**i. disseminating information;**

- Threat level changes are disseminated to all audiences. Perhaps there is a need for a system to provide more specific information to critical infrastructure and key resources and government agencies with jurisdiction.

**ii. implementing “protective measures;”**

**iii. creating common vocabulary, context, and structure for discussion about threats and appropriate courses of action; and**

- More frequent testing of the system would raise consciousness regarding appropriate actions at each threat level. This could be modeled on the “emergency broadcast testing” system.
- HSAS uses different vocabulary than MARSEC/COOP/COGCON. Should the three systems use a common structure (colors or numeric with the same structure – low to high or high to low)?
- Develop a table – similar to that for the COGCON levels – that delineates specific actions at each HSAS level. This currently exists for the general population in the *Citizen Guidance on the Homeland Security Advisory System*.

**iv. informing and facilitating decisions appropriate to different levels of government and private citizens?**

- Alerts could be stratified/customized for different audiences.
- Alerts should be broadcast using the Common Alerting Protocol.

**v. Should there be alternative purposes?**

GSA→A major change that would increase the effectiveness of the system would be to incorporate sub threat mitigation requirements under each advisory level. These measures would identify baseline requirements that each department an agency would be responsible to implement allowing those departments an agencies that fit the target set mold to adjust there defensive posture to a level that commensurate with the forecasted threat.

b. Is the purpose in HSPD-3, as stated, the right purpose regarding:

- i. disseminating information;
- ii. implementing “protective measures;”
- iii. creating common vocabulary, context, and structure for discussion about threats and appropriate courses of action; and
- iv. informing and facilitating decisions appropriate to different levels of government and private citizens?
- v. Should there be alternative purposes?

DoD → Yes. In addition to those things, the HSAS system should clearly distinguish between a heightened, specific threat and a general threat (credible or not credible). The bottom line is that HSAS should help us *turn off* government activity and public anxiety as well as turn it on.

GSA → In a general sense, the HSPD stated purpose meets the spirit and intent of the system, however department and agencies should be given a baseline requirement at each level that still affords them the opportunity to enhance the requirement as it pertains to the forecasted threat at the same time achieving a unified escalation in the outward appearance of their security posture.

c. What changes, if any, are needed in the design/architecture of the HSAS?  
Please consider the:

- i. type of information communicated;
- ii. audience(s) for information communicated;
- iii. mechanisms/means of communications;
- iv. operation of the system; and
- v. intended actions to be triggered (to implement protective measures).

DoD → HSAS needs three changes in design and architecture. 1) HSAS needs clear criteria in terms of triggers and thresholds for each HSAS level. 2) HSAS needs escalating criteria for its higher levels and a process that *automatically* returns the system to its lowest level unless those criteria can be met on a regularly recurring basis (e.g., HSAS level will return to blue on the first of every month unless DHS can concretely

USDA →

i. **type of information communicated;**

- Need to balance information provided with maintaining the integrity of intelligence/law enforcement investigations.

ii. **audience(s) for information communicated;**

- Two Audiences – Public and government/business. Notifying and creating a need for action in the public is a different than doing so for government/business. Consider public needs and messaging separately from government/business.

Public notification needs to consider sufficiency of information to drive the desired action.

- Regional versus National - Need to balance the costs of raising the threat level nationally with the impact to intelligence/law enforcement operations if the threat level is raised regionally.
- Sector-specific - Need to balance the costs of raising the threat level nationally with the impact to intelligence/law enforcement operations if the threat level is raised for specific sectors.

**iii. mechanisms/means of communications;**

- Alerts should take advantage of social and professional networking sites.

**iv. operation of the system; and**

- Reduce the five stages to three.

**v. intended actions to be triggered (to implement protective measures).**

- Simple terms should be used in an actionable format.

GSA → The system should be designed to get specific threat information not only to senior leadership but also to the operations level in order to facilitate timely implementation of specific mitigative measures to reduce the potential impact of the forecasted threat.

- **For any improvements or changes proposed, what are the implications to:**
  - security;**
  - costs;**
  - law/authorities;**
  - sociology;**
  - operations/governance; and**
  - other factors?**

DoD → All of these recommendations have huge cost implications. If the U.S. government will actually take actions based on HSAS changes, that will be incredibly expensive. Yet, if HSAS doesn't drive U.S. government operations, one might ask: what does it do? And if cost doesn't increase as the HSAS level increases, the federal government never has any incentive to lower the HSAS level (since it will be politically convenient for the HSAS level to be high if an attack occurs so that we can claim we warned the public and politically inconvenient for the HSAS level to be low if an attack occurs).

Tying U.S. government operations to HSAS level changes will measurably increase U.S. security by giving us a clear and routine process for responding to threats.

Tying the operations of other agencies to the HSAS level will diminish their authorities in the homeland security arena vis a vis the Secretary of Homeland Security, but it will appropriately increase her stature as the domestic incident manager. The key is to make the HSAS declaration and

review process clear, with clear guidelines, and requirements for consultation with other key departments and agencies so that the Secretary can increase HSAS, but not without really proving there is a need to do so. It may be that to circumvent the authorities issue, we should escalate HSAS level changes to the President himself.

Sociology: These recommendations will help with public complacency by making it much more difficult for the U.S. government to increase the threat level. That means the public will know that there really is a threat when HSAS goes up and can implement appropriate preparedness measures.

## **USDA→**

### **a. security;**

- Need to balance integrity of intelligence/law enforcement operations with need to provide sufficient information to drive desired actions.

### **b. costs;**

- Costs associated with updating/replacing printed media with changes, public service announcements/education for changes.

### **c. law/authorities;**

- No changes to laws, revision of HSPD-3

### **d. sociology;**

- Reducing stages from five to three – Positive impact that baseline is normal, should assist in making public more responsive to changes in the stages.
- Use of social networking sites – may increase confusion as some formats allow for limited message length. Increases awareness among certain segments of the population.

### **e. operations/governance; and**

- No associated implications

### **f. other factors?**

- The current system does work, it should be kept in place until a replacement system is complete and ready to implement.

GSA→The overall impact to the below line items should be minimum as the improvement will involve specific threat dissemination (information) and baseline mitigation measures development. Most of the cost will most likely be borne by the department and agencies as they develop specific offensive and defensive measures to employ for each HSAS level, as well as local measures that are unique to that department and agency as it pertains to a defined threat.

# Synthesized Interagency Input about the HSAS

NOTE: The following is a summary of DHS input provided by various federal agencies regarding the Key Study Questions about the Homeland Security Advisory System (HSAS).

## Themes: Strengths of the System

- *Simplicity and common vocabulary*
  - 3 agencies noted the simplicity of the system.
    - “It provides a common vocabulary and a general sense of the level of threat.”
    - Focus on a common vocabulary was noted. “HSAS provides an already familiar methodology for threat communication that is conceptually easy to understand.”
    - Talked about HSAS providing a “uniformed readiness baseline.”

## Themes: Weaknesses of the System

- *Colors have no meaning anymore*
  - Amongst the major themes in this section is how the colors do not convey any real meaning anymore.
    - “The colors seem to have lost meaning, particularly since the nation has not come down from yellow since the system’s inception.”
    - Explains that the system has only been between yellow and red since system’s creation. (blue and green not used).
    - Too many levels; should reduce to three.
- *Need for more specificity*
  - Another common theme is the need for warnings to be more specific
    - Mentions the need to distinguish between specific and general threats.
    - System needs to issue sector and regional specific warnings.
    - “The specificity of available threat information will have a significant impact on implementing program-specific actions, notifications, and procedures.”
    - Need to have more concrete protective measures.
- *Defining the levels better*
  - Two agencies discuss the need to define the levels with clearer criteria
    - “HSAS needs clear criteria in terms of triggers and thresholds for each HSAS level.”
    - Comment about need to define risk more clearly
- *Public reaction to the system*
  - Comments about the system creating public anxiety.
    - Suggested a bifurcated system for public and responders
  - Comment about the belief that the system’s main audience should be the public

- Suggestion that perhaps a bifurcated system, in which “more specific information to critical infrastructure and key resources and government agencies with jurisdiction.”
- *Costs of implementing the system*
  - Two agencies expressed concern over the costs of the current system and potential future costs.
    - If the U.S. government will actually take actions based on HSAS changes that will be incredibly expensive.”
    - Huge costs of maintaining orange level.

***Other interesting notes:***

- One proposal for a way in which the levels would automatically return to their lowest point unless certain threat thresholds are met.
- “The key to any change should focus on protective measures, rather than a color code.”
- Need to use technology such as social networking sites to issue alerts.

Attachments:

[Compiled Responses to Key Study Questions]

[Additional Comments from the Interagency

## **Additional Comments from the Interagency:**

### **Compiled from Emails or from Documents sent to DHS**

**Background:** The below comments were compiled from responses to Key Study Questions about the Homeland Security Advisory System. All wording is original from the responsible agency, with only some formatting changes to fit this page. All grammar and syntax is original to the authoring agency.

### **Homeland Security Advisory System (HSAS)- EPA input to Request for Comments**

#### **EPA:**

In response to the DRG request for Comments on the Homeland Security Advisory System (HSAS) for the 60-day DHS review, below please find the input from the Environmental Protection Agency (EPA):

#### **-What (if anything) should replace the system?**

Our opinion is that the system does not need to be replaced, instead it should be refined. The current HSAS provides an already familiar methodology for threat communication that is conceptually easy to understand. A color-coded system is simple, requires little by way of explanation to the general public and helps create a common vocabulary for educating and impacting public behavior. The enhancement/refinement should focus on providing clearer definition of risk category (i.e., general, significant, high, or severe), defining the anticipated actions of the federal government, and streamlining the threat levels in order to better reflect current and anticipated future conditions.

#### **-Who is the audience/ target for the information communicated?**

We believe that the main target audience for HSAS information should be the general public and potentially impacted industry/economic sectors. The government sector is also an audience, but should have alternative systems in place to be kept better informed on necessary or recommended actions.

#### **-What type of information should be disseminated from the system?**

The information provided by the system should be simple to understand for the public and, where appropriate, provide recommended protective actions.

Departments and Agency's should have more sophisticated systems for disseminating specific threat information relevant to their program areas.

## **-What are the intended actions to be triggered?**

Changes in the HSAS threat level impact the readiness posture of the government sector entities as well as those of the potentially impacted industry/economic sectors. The specificity of available threat information will have a significant impact on implementing program-specific actions, notifications, and procedures.

DOT provides the following input regarding the HSAS:

The concept of an advisory system for Homeland Security seemed appropriate after 9-11. The idea that the executive branch of government would coordinate its protective measures is sound. When HSPD-3 was implemented, HSAS became recognized based on colors and not the corresponding protective measures. When it was first implemented nationwide, it became clear that it was quite expensive to maintain orange level. The impact was felt heavily by States, local jurisdictions and the private sector.

The key to any change should focus on protective measures, rather than a color code. The colors seem to have lost meaning, particularly since the nation has not come down from yellow since the system's inception, and the aviation sector has been at orange since August 2006. For this reason, we recommend considering establishing protective measure norms for the steady state and enhanced levels that can be used selectively based on the conditions and the sector or geographic region to which is should be applied. We also suggest that when enhanced protective measures are applied, there should be a corresponding exit strategy that takes into consideration sustainability issues, such as cost. One of the largest costs in the transportation sector is the congestion caused by increased security. Because of the intermodal nature of transportation, congestion or backup in any particular mode of transportation affects other transportation modes.

There should also be a corresponding public alert and warning facet that translates the government's actions into useful public information whenever a change occurs.

There have been recurring difficulties related to making decisions on changing the alert status. There should be equal and informed involvement from all appropriate agencies in any such decisions, rather than solely the two agencies identified in HSPD-3. This is critical to quality decision-making.

## Response from Professor Philip Zimbardo

Philip G. Zimbardo, Ph.D.  
Professor Emeritus, Psychology  
Stanford University  
Stanford CA 94305

July 26, 2009

Dear Jeff Karonis:

Thank you for the opportunity to contribute to the discussion surrounding Secretary Napolitano's review of the Homeland Security Advisory System and the color- coded alert system.

It has been my public position, in published writings and speeches over the past 5 years, that the terror alert system as practiced in the United States is less than worthless, and needs to be thoroughly revised. That revision must be based on our understanding of effective emergency warning systems and the psychological analysis of how best to motivate citizens for impending dangers facing them.

I am the Director of the Stanford's Center for Interdisciplinary Research, Education, and Policy (CIPERT). I am also a senior professor at the Monterey Naval Postgraduate School, teaching a course on the Psychology of Terrorism since 2002 to a diverse body of master's program students (in Homeland Security and Defense). Among them many first responders in state wide departments of police and fire, FBI, CIA, Coast Guard, Central Command, Governor's policy spokespersons and a variety of others. We have regularly discussed the utility and futility of our nation's terror alert system and the need for some new program that is more honest, transparent and achieves it purpose without deception.

I am attaching an article I wrote on this topic a couple of years ago with my political psychologist colleague, Dr. Rose McDermott (Professor at Brown University, who I also copy on this note):  
McDermott, R. & Zimbardo, P. (2006). The Psychology of Terrorist Alarms. In *The Psychology of Terrorism*. B. Bonger, L. Beutler, J. Breckenridge, & P.G. Zimbardo (Eds.). New York: Oxford Press.

I believe that this article should be useful for your evaluation. Based on our research, we believe that the current color- coded system should be discarded and not salvaged in any way. It provides no useful information to the general public or our service corps because since its inception, it is a two-value system pretending to be an alert continuum. The alert level has never dropped below orange—which it is now for the past 18 months at least! Because a level of red equates to an actual attack, there is in reality only one color, since no politician has proved willing to accept the political consequences of reducing the presumed threat level even to a more modest yellow.

In reality, then, the current color- coded system offers no real or usable information about the nature of potential threats. This system has clearly evolved over time to be used primarily for political ideology, and contains no effective psychological, practical, or even political efficacy. Polls reveal the public does not know or even remember the risk associated with the colors, many believe

it has been politically motivated to maintain a high threat level to promote citizen vulnerability and thus support for the Bush administration's "War on Terror." Research also reveals that in one sense these alerts have served to do the terrorists' work for them because it costs a huge sum of funds to maintain the nation on high alert, and stress levels accelerate among many of our citizens, so there really is no need for an actual attack if a virtual one has such negative impacts on our nation. Other research reveals a reason for cynicism about the use of the color-coded alarm system: Bush's popularity ratings increased by 3-4 % following each changed color level.

In addition to these wasted costs and increased sense of national vulnerability-- when we need our citizens to be resilient—there has been a loss of confidence in the government in general. In part, this can be traced to the non-obvious fact that after any threat level was changed, any of the earlier verbal threat messages or the color-coded ones, **THERE HAS NEVER BEEN A PUBLIC DEBRIEFING**, by a national official, to explain the reason for reducing the threat alert. That must be changed,

I believe it is the task of Secretary Napolitano to be responsible for such national assurances following the extended absence of a predicted threat. The public needs a trustworthy communicator of these vital messages.

Moreover, she or someone with credibility in the current administration, needs to issue a statement in layman's language of an impending terror threat—based on the best available information—and noting the former color-coded system has been dropped because it proved not be sufficiently informative for the public.

The key features of any alert alarm emergency warning are: a) a credible communicator issues the warning; b) the warning is as specific as possible as to region, type of emergency (not anywhere any time), etc.; c) citizens must be given actions to engage in to prepare for the emergency response (not the BUSH- BOLO, "BE ON THE LOOK OUT" for evil men doing bad deeds), and d) the public must be engaged as active participants in this drama, not passive pawns of political intrigue or TSA expediencies.

Also alerts can go to national and local first responders and other officials, and not necessarily to citizens when there is little citizens can do given a vague alert. Also, as noted earlier, when the threat level lowers, the Secretary or some other high level issue must issue a statement to that effect at that time as well.

My colleague and I would be happy to provide additional feedback and information on the futile nature of the current system, as well as offer other suggestions for a more effective system, if you so desire. Thank you for consideration of our input.

Cordially,



Philip Zimbardo

See also my earlier critical writings on the warning system.

- Zimbardo, P. G. (2001, December 30). Psychology of terrorism: Mind games, mind healing. *San Francisco Chronicle*, D6.
- Zimbardo, P. G. (2003, May/June). Phantom menace: Is Washington terrorizing us more than Al-Qaida? *Psychology Today*, 36, 34-36.
- Plous, S. & Zimbardo, P. G., (2004). Using social science to reduce terrorism. *The Chronicle of Higher Education*, B9-B10.
- Zimbardo, P. G. (2006). Foreword: The political psychology of terrorist alarms. In *Collateral Damage: The Psychological Consequences of America's War on Terrorism*. P. R. Kimmel & C. E. Stout (Eds.). (Pp. vii-x) Westport, CT: Praeger.



Department of Homeland Security  
Assistant Secretary for Public Affairs

## **Synthesized Public Communications Stakeholder Summary**

### **HOMELAND SECURITY ADVISORY SYSTEM REVIEW**

NOTE: The following is a summary of DHS input provided by various communications experts.

*The effectiveness and the public acceptance of any homeland security advisory system will depend on how well, in the minds of the average American, the system is framed within a perception of greater trust and confidence in government facilitated by increased citizen engagement. Our data strongly suggest that simply improving risk messaging, albeit a critical task, or clarifying citizen guidance about the evolving advisory program, will not be sufficient to restore public trust and confidence in warnings, crisis instructions, or efforts to protect the nation from terrorism.<sup>2</sup>*

#### **1. Summary.**

Dr James Breckenridge, a noted terrorism researcher at Stanford University, captured the essential communications challenge with any terrorism warning system, and how it could be effectively employed in our nation. *Trust* is the essential component to the success of any HSAS system. Perfect messaging, color codes, or adjective threat advisories will not be effective without the public's confidence in the system and those delivering the message. This is both a public perception and finding which is echoed in communications stakeholder responses received by DHS Public Affairs. From these respondent comments we have identified key trends that may serve as *guideposts* for the HSAS Review and how communications can be more effectively integrated within a system and executed to serve the information needs of our citizens.

The guideposts we identified from stakeholders and public comments are listed below and discussed in detail in subsequent sections in this paper.

- There must be public trust and confidence in authorities conveying threat information
- Preparedness and public education about threats and public action are essential
- There must be specificity in what is conveyed to the public about the threat
- New media must be integrated within any new advisory system

---

<sup>2</sup> Dr James Breckenridge, Associate Director, Center for Interdisciplinary Policy, Education, and Research on Terrorism, Stanford University and Navy PG School, letter to DHS Public Affairs Aug 7, 2009.

## 2. Stakeholder Groups and Methodology.

DHS Public Affairs cast a wide solicitation for comments on public communications. This was critical inasmuch as public communications is an essential component for any HSAS type system, and has also been cited as a deficiency with our existing system. Our stakeholder solicitations were varied and we were very pleased with the constructive

comments provided by our respondents. We have submitted several stakeholder comment packages with this summary to the Review panel as they provide a wealth of useful perspectives for consideration.

Our key stakeholder groups are summarized below:

- **Academic Community.** Risk communications theorists, media studies, former media in academic positions. Excellent feedback was received from respondents.
- **Media.** We extended the offer to several national TV news networks and major print media to provide comments on the HSAS and recommendations for improvements. This was done in the spirit of transparency and because the media is, in many respects, a customer and user of the HSAS. Media ethics limitations precluded participation with the exception of one cable TV news network. We balanced this with former media who willingly participated in the review.
- **Practitioners.** This group includes professional public affairs staff from Federal, state, local, and private sector positions.
- **New Media.** We reached out to new media representatives currently leading national and worldwide social media enterprises. We also included blog writers who continue to gain significant influence in our media and in affecting public opinion.
- **Public Comments.** To assure transparency, DHS Public Affairs established a comment website to allow the public to submit recommendations and comments about HSAS and the review. This provided a very useful citizen perspective.

## 3. Public Trust and Confidence

*On April 18, 1775, patriot Paul Revere rode his horse on his famous “midnight ride” from Boston harbor toward Lexington, warning local colonial leaders along the way that the British, the redcoats, were coming. Revere’s warning was effective for four reasons: (1) he was known to be a highly credible communicator, both expert and trustworthy; (2) his alarm was focused on a specific anticipated event; (3) it was designed to motivate citizens to act; and (4) it called for a concrete set of actions....This Paul Revere paradigm for successful dissemination of public alarms is supported by contemporary psychological research.<sup>3</sup>*

As noted in the initial comments on this paper trust is the essential component to a viable and effective threat warning system. Many experts and articles on HSAS point to the *lack* of trust in

---

<sup>3</sup> Dr Phil Zimbardo, Director of the Stanford University Center for Interdisciplinary Research, Education, and Policy (CIPERT), excerpted comments to DHS on the HSAS, July 26, 2009.

the current system as a significant element in its ineffectiveness. Moreover, our data from the public respondents show that 15% specifically cited lack of trust in the government's use of the existing HSAS as a major concern. David Ropeik, an experienced risk communications specialist, educator, and advisor to senior US Government leaders, explained how the current HSAS is flawed in this regard and actually undermines the intention of the government's communications.

*The [current HSAS] is far too general, and in the context of good risk communication, that generality leads to greater uncertainty, which contributes to greater fear. Also, the general nature of the information tends to breed skepticism and doubt, and **mistrust** in government officials. That further feeds fear, fueling fearful responses which contribute to, rather than combats, the psychological effect of terrorism, which is, after all, one of its aims.<sup>4</sup>*

Building, or rather *re-building* public trust and confidence in a new HSAS will be the primary task, in our view, for communicators and designers of a new system. This trust can be gained through transparency, confidence in the leaders and communicators providing the information, and in public education about the advisory system *before* a threat is announced. Risk communications is a key resource that will assist in the effective deployment of a new advisory system.

*Risk communications is an intrinsic part of managing how people behave when they are afraid, and that is a fundamental part of managing the response to terrorism. The implication here is that changes to the HSAS system have to be thought through and integrated from the top down, not from the communications staff up.<sup>5</sup>*

#### **Trust and Confidence -- Perspectives and Recommendations**

- **There must be public trust and confidence in authorities conveying threat information**
- Threat advisory announcements should be clear, transparent with respect to the threat, and explain why authorities are taking this action.
- Consideration should be given to any new advisory system to include feedback and technological resources which allow authorities to gain insight into public awareness of the threat and allow adjustments to the communications advisory if issues are unclear or require updating.

#### **4. Preparedness and Public Education**

*Decades of empirical research on public preparedness leads disaster social scientists to claim that 'we know how to reach the public, how to teach the public, and how to motivate preparedness activity.' It is imperative that public education become an integral part of a warning system.<sup>6</sup>*

It has been recognized since 9-11 that public preparedness for terrorism is a vital component and challenge for all leaders and homeland security officials. To this end, the Ready Campaign

<sup>4</sup> David Ropeik, HSAS Risk Communications Respondent to DHS, Aug 2009.

<sup>5</sup> David Ropeik.

<sup>6</sup> Dr Jeannette Sutton, Natural Hazards Center (University of Colorado), comments to DHS on the HSAS, Aug 7, 2009.

(Ready.gov), established in 2003 as a flagship program within the new Department of Homeland Security, has sought to increase public knowledge about all-hazards threats and what people should know and do before an incident occurs. This program was not directly linked to the HSAS but supported general communications and was frequently cited by principals as they informed the public about threats and what they should do. It is clear from our respondent comments that public education about threats and a national advisory system will enhance the effectiveness of announcements and public acceptance and trust. The frustration of a citizen respondent, who also serves in an emergency role, reflects the need to enhance public knowledge about threat advisory systems.

*From my perspective, the existing DHS color code system was implemented with great intentions, although the lack of a detailed on-going public education campaign missed the mark. Consistently, citizens from my community will ask me what are the trigger points, or bench marks to change the color, but more importantly, what actions should they be taking in their personal lives should that threat level change? Unfortunately, I can't give them any real clear guidance.<sup>7</sup>*

### **Preparedness and Public Education -- Perspectives and Recommendations**

- **Preparedness and public education about threats and public action are essential components**
- The Review team should closely assess the results of the 2008 CHDS/CIPERT American Perceptions Study on Terrorism. This study provides data that can assist in the development of a new HSAS and ensure that public information expectations are incorporated.
- A new advisory system should include a continuing public education communications component to assure public awareness and involvement.
- A new advisory system should also include a robust public rollout effort conducted on a nationwide basis, to assure that citizens, the private sector, schools, etc are fully apprised of the new system.
- The Ready.gov program and supporting state programs should be evaluated as potential resources for public education on the new advisory system.

## **5. Specificity**

*The HSAS should take into account more than fifty years of empirical research on the design of effective warning messages. Disaster social scientists have conducted research that have taken into account and analyzed all of the known factors that affect one's behavior in response to a hazard or threat. The most salient issues which increase public responses to a warning message are the **content** of the warning message itself and its **repetition**.<sup>8</sup>*

Specificity with threat information is critical. Risk communications, which are universally accepted and scientifically founded procedures, reinforce that point. However, the lack of specificity with threat information has been habitually cited as a fault of the existing HSAS

<sup>7</sup> Citizen HSAS respondent to DHS website, July 26, 2009.

<sup>8</sup> Dr Jeannette Sutton

system. To be fair, certain security limits preclude disclosure of all threat information, and that challenge is not likely to go away. What is sought is a balance between what the public can be told and what they need to do in response to this threat information. The 2004 Orange threat change due to the financial district threats is a good example of balancing security but still providing transparency for all, including the citizens and occupants of potentially targeted buildings.

Dr Jeannette Sutton, a researcher at the Natural Disaster Center and noted expert on disaster communications, noted that the current HSAS system fails in providing the public with the information they need.

*[HSAS] does not provide specific information or advice regarding appropriate measures and countermeasures that may be taken in response to the threat or risk.....In addition, it fails to provide sufficient information to the public that will enable them to prepare for future events.<sup>9</sup>*

Other comments from respondents echo this concern, including state public information officers. We also noted that 41% of citizen respondents to the DHS HSAS website cited the lack of specificity in the current HSAS process as a major concern. This reinforces the need for communicators to be advocates of transparency, as threats and as any new threat advisory system is developed and presented to our citizens.

#### **Specificity -- Perspectives and Recommendations**

- **There must be specificity in what is conveyed to the public about the threat.**
- Threat information can be presented through different means than colors or risk levels – it can be communicated effectively by: (1) using credible communicators, (2) providing specific information about the threat or situation, (3) motivating citizens to act and be involved, and (4) providing them with actions they can take to prepare.
- DHS and supporting official homeland security websites, such as state and local, should provide detailed information on threat information, recommendations and/or direction on preparedness, and a feedback process that allows the public to communicate their concerns or questions to authorities about the threat.
- As the threat diminishes, authorities should promptly explain why and what caused the change in the situation, and what public action should be as a result.

## **6. Public Comments and Trends**

Public comments to the DHS Public Affairs website were largely constructive and showed that citizens have a keen interest in a national alerting and warning system, and want to help improve it. We reviewed all public comments and determined that the below areas represented the clearest trend indicators. While this is not scientifically based since the sample population voluntarily offered their comments it does reflect an apparent pattern that is echoed in

---

<sup>9</sup> Dr Jeannette Sutton.

professional critiques of the existing HSAS and need for improvement. The comments on the need for increased specificity were important because they reflected citizens who were both for and against the existing HSAS: Tell the public more, tell them what they should, do, and tell them when and why the threat has diminished. Also of note is the rather high percentage of respondents expressing mistrust of the current HSAS and citing its vagueness as contributing to complacency about threat information.

<b>DHS HSAS Public Website Comment Trends (127 Respondents)</b>	
<b>Change the existing HSAS (115)</b>	<b>74%</b>
<b>Retain the existing HSAS (31)</b>	<b>19%</b>
<b>Need for more specificity in HSAS alerts</b>	<b>41%</b>
<b>Don't trust HSAS (political manipulation)</b>	<b>15%</b>
<b>Current HSAS is fostering complacency</b>	<b>14%</b>

## 7. New Media

*One key question for DHS is emergency communication: how best to get urgent, actionable information to everybody who needs to know. This is the same question a university president or a mayor faces. Social media will be paramount: More people get urgent information via cell phone and Twitter (or whatever replaces it) than via newspapers or even television.<sup>10</sup>*

The Obama Administration has aggressively initiated efforts to integrate social media to enhance transparency between government and citizens. This is a new effort and will enable the government to reach a much larger audience in a shorter period without depending on conventional media resources, such as TV and radio. To complement the HSAS Review DHS reached out to key social and new media enterprises in the nation and they are participating as stakeholders in our communications survey. Stakeholders include GOOGLE, Facebook, Twitter, and YouTube. Their focus is determining how they can support dissemination of threat information and how it can be integrated within their products.

The comments from new media stakeholders have not yet been received. We will provide those when they are received and we can summarize their contributions and suggestions.

Aside from that national-level feedback we are fully aware that new personal technology devices can have a major role in conveying threat information. This has been demonstrated on college campuses and school systems operating under criminal threat situations. How these lessons learned and technology already in use can be employed with a new advisory system is both a

<sup>10</sup> Dr Peter Sandman, Risk Communications expert and DHS HSAS respondent, July 2009.

challenge and a potential resource of great significance. To reinforce that point, the New York State Public Information Officer for homeland security noted the following:

*Allow the public to sign up to receive these alerts through the various devices (cell phone, PDA, blackberry, pager, etc). Something similar to NY-ALERT, New York State's alert and notification system ([www.nyalert.gov](http://www.nyalert.gov)) and receive information that means something to them. I.e., if level goes to Orange, say that and what public should do.<sup>11</sup>*

Websites are valuable resources for conveying threat information. To this end, several respondents noted how blogs can be another complementary information resource. DHS Public Affairs has already established a departmental blog to amplify information on department activities and this would likely be employed during a threat situation. One of our communications respondents noted this as a potential resource.

*Maybe the [DHS] website should include a blog, with fresh information daily from the Secretary and other officials. This shouldn't be about public relations, but should be real information that is of interest – or, better, importance to the public and the media. Let the public provide input, and respond to it.<sup>12</sup>*

### **New Media -- Perspectives and Recommendations**

- **New media must be integrated within any new advisory system.**
- A new advisory system should be assessed for its ability to assimilate with existing public communications technology and adapt its operating procedures to new platforms with advances capabilities and innovation.
- Blogs offer a potential new wealth of capability with a threat advisory system and directly involve the public – a key requirement to the success of any risk communications strategy.

### **Key Communications Stakeholder Respondents**

Dr James Breckendridge letter to DHS HSAS Review of Aug 7, 2009  
Dr Jeannette Sutton email to DHS HSAS Review of Aug 7, 2009  
Dr Peter Sandman email to DHS HSAS Review of July, 2009  
Dr Phillip Zimbardo email to DHS HSAS Review of July 2009  
Randy Atkins, National Academies email to DHS HSAS Review of Aug 7, 2009  
David Ropeik email to DHS HSAS Review of Aug 5, 2009  
Jay Alan, California Homeland Security Communications email of Aug 6, 2009  
Rich Cooper email to DHS HSAS Review of Aug 2009  
DHS Science and Technology notes and comments on HSAS Human factors  
FEMA External Affairs DHS HSAS Review of Aug 09

<sup>11</sup>Dennis Mikhalski, NY State PIO, HSAS Review comments, July 2009.

<sup>12</sup>Randy Atkins, Communications Director for the National Academies, DHS HSAS respondent, July 2009.

# Synthesized DHS S&T Comments from Randy Beardsworth

## ***Human Systems Integration Notes:***

### **(1) HF Issues Identified for the Homeland Security Advisory System**

When considering Human Factors issues across the different components (colors, words, and phrases) of the HSAS

- May not be an effective hazard communication tool
- Colors were not well associated with the threat levels when asked to sort colors according to the level of the threat
- Certain colors (e.g., red and orange) are not differentiated on the hazard continuum; certain colors indicate a greater level of hazard than others (e.g., yellow and red vs. blue and green)
- Individuals are generally better able to understand the level of threat based on the associated words (e.g., often confused guarded and low conditions; as well as elevated and guarded conditions)
- The phrasing used in the system tends to be the most helpful when it comes to helping individuals understand threat levels (e.g., “most frequently confused significant and high risk of terrorist attacks”)
- Recommendations for an appropriate color scheme, signal words, and phrasing to support information understanding

#### **Source**

**Mayhorn, Wogalter, and Shaver (Fall 2004). Ergonomics in Design**

### **(2) HF Issues identified for Pictorial Warning/Safety Symbols**

- Recommendation for a DHS Public Education Framework (public awareness campaign)
- Symbols should communicate the nature of the hazard and the behavior necessary to avoid injury
- Study demonstrated that 79% of DHS pictorial safety symbols (according to study participants) are unacceptable for communicating hazard-related information
- Some concepts are not amenable to pictorial communication—may be the case that simplified text is preferred due to abstract, complex nature of message
  - e.g., If you see signs of a chemical attack, try to define the impact area or where the chemical is coming from was accurately comprehended by 33% of the participants)

#### **Source**

**Mayhorn, Wogalter, and Bell (Fall 2004). Ergonomics in Design**

## **START document notes\*:**

START would offer that social-science research has identified characteristics of effective warning systems and warnings, from an all-hazards perspective. Among the conclusions of this research are:

- ~ Do not try to convince people they are at risk: It has no good effect on public preparedness or avoidance behavior.
- ~ Provide public information from as many different sources and with as much consistency across all messages as possible.
- ~ Distribute information over as many different channels as possible, as often as possible and over extended periods of time.
- ~ Tell people what they should do to prepare and where to find out more about how to do it.
- ~ Tell people how their actions can reduce their losses, don't give them risk estimates.

## **Community Resilience Summary Notes\*:**

### SUMMARY NOTES

Susan Cutter's address "The Vulnerability of Science and the Science of Vulnerability" (p. 7, 2<sup>nd</sup> column) explains the difference between "expert" and "lay" judgments with an oft-quoted observation from a National Academies study that "Risk perception research found that public understanding of risk was not flawed or wrong; rather, risks were more broadly defined by the public, who took into account some of the societal implications of accepting the risks in their acceptability/unacceptability judgment. ... In other words societal selection of what risks or hazards to emphasize and which ones to ignore often reflected moral, political, and economic choices that were themselves value-laden and socially constructed."

Baruch Fischhoff, et al, "Expert Model of Risk" (Chapter 3 from the book *Risk Communication: A Mental Model Approach*), provides the best quick and dirty method I have seen of conducting risk assessment according to the desired outcome. It employs influence diagrams to explain how to identify and sequence the cause and effect relationships for constructing outcome-based risk assessments.

Lerner, Gonzalez, et al "Effects of fear and anger on perceived risks of terrorism."

This is a technical article from the journal *Psychological Science*. The summary describes the article's main point:

"A field experiment using a nationally representative sample and a multi-method approach, found that fear and anger altered beliefs and attitudes regarding matters of national interest. Experiencing more anger triggered more optimistic beliefs; experiencing more fear triggered greater pessimism. These effects held across a range of risks (terror and non-terror related) and with both a verbal response scale and a more analytical probability response scale. ... As has been found previously, respondents saw themselves as less vulnerable to risks than the average American, and less likely to take precautionary measures. However, these judgments of relative risk did not reflect unrealistic

optimism, in an absolute sense. Some risk estimates (e.g. for the average American being a victim of violent crime) reflect pronounced pessimism, considering historical risk rates. Other risk judgments [from data collected a year after 9/11] ... estimated a 20% chance of being hurt in a terror attack for themselves, and a 48% chance for the average American.” (Conclusions, p. 148).

Matheny, “Reducing the Risk of Human Extinction.”

Finally, and mostly for amusement, I provide Matheny’s article from the Society for Risk Analysis on “Reducing the Risk of Human Extinction.” This will probably have no utility for the problem at hand, but I actually use this article in teaching risk assessment because it demonstrates in a serious scientific journal that it is possible to bound any problem and, having done so, to begin rationally identifying alternative courses of action. It’s worth examining simply to put government problems in perspective.

I also recommend anything written by Amanda Ripley, for the simple reason that her observations about risk and preparedness resonate with the American public in a way that no academic researcher or expert in risk assessment does.

## **Suggestion from HSAC Member, Kareem Shora**

### ***Current drawbacks:***

The current HSAS is too broad and "fear-centric." For example, the "Yellow" which is meant to represent the "middle of the road" situation is defined as representative of a "Significant Risk of Terrorist attack." When the "Yellow" becomes the norm, as has been the case since the HSAS was practically implemented, the HSAS loses credibility and the public no longer takes it seriously. The current system also fails to provide specific information and guidance to state and local first-responders and the **general population**.

### ***Constructive suggestions:***

While the color combination may remain, given the costs associated with a complete change of the HSAS, the following improvements may be helpful:

- 1) Include numbers - easier to include, level 1 (green) to level 5 (red). While this will not address the "fear-centric" definition now associated with the HSAS, it will help the public relate more closely to the HSAS given that most "threat alert systems" are numerically-based (i.e. Hurricanes, Tornadoes, Earthquakes, etc.)
- 2) Revamp the descriptions / definitions for the categories to be more specific and representative of the situation; the current descriptions are too broad. The definitions should be descriptive enough to allow for a clear understanding of the current situation / environment and more detailed in order to alleviate the "fear-centric" approach of the current HSAS.
- 3) Include instructions for the public under each category. Include things to look out for, things to consider, how to react in the event of an attack based on the current HSAS level. Without disclosing sensitive information, this will help the public understand why the HSAS level has changed / remained at a certain color / number, and provide realistic general guidance on security expectations and steps each person can take to both help protect the homeland while maintaining the normality of their daily lives.
- 4) Include what general steps different government agencies (federal, state, and local) are taking or need to take under each of those HSAS categories. This will help alleviate unrealistic fears, provide guidance to the general public, and also assist first-responders on the state and local levels to know how to react and what steps to take. It is clear that under the current HSAS there is no consistent set of specific standards for state and local first-responders to follow. These general steps would be very helpful for both local communities, first-responders, and individual families.

### ***Conclusion:***

The current HSAS' fear-based approach has failed and has created confusion and mistrust by many first-responders and the general population. The perception appears to be that the HSAS is a stand-alone symbolic tool that has failed to provide enough information and guidance to these stakeholders. In addition to the recommendations mentioned above, the HSAS should be looped in to other DHS preparedness programs such as the DHS Preparedness website and Ready.gov. Taking these steps and publicizing them would go a long way in improving people's trust in the new HSAS as a reliable and realistic tool which provides specific information and guidance.

# Synthesized Private Sector Comments

NOTE: The following is a summary of DHS input provided by various federal agencies regarding the Key Study Questions about the Homeland Security Advisory System (HSAS).

## **General**

- Given the limited representation of the private sector on the task force, members of the private sector would like an opportunity to take an ongoing roll through the work of the task force, even if feedback would have to be provided on a very short timeline.
- Some industry representatives suggest a routine review of HSAS to design appropriate measures rather than being prescriptive.
- Members of the academic community have studied the HSAS and its effects as well as all-hazards warning systems and believe the task force could benefit from their work.
- The current HSAS system provides a single point of reference that is easy and can get attention when necessary.
- HSAS is neither dynamic nor responsive enough. A more fluid system may help HSAS meet its true intent by updating regularly with concrete concerns/issues/threats/alerts. Revisions can be made with each change in threat level, but guidance should be reviewed at least monthly.
- It may be possible to make changes to HSAS without adding significant cost as proposed changes primarily involve utilizing and sharing threat analysis already being conducted.
- The system itself is not broken, but the vehicle by which it is communicated is not supported by an education program to turn the HSAS information into actionable results.
- The system is, in practice, too risk-based. HSAS must do a more effective job differentiating between risk-based concerns and threat-based concerns.
- More consideration should be given to the evolving homeland security landscape. This includes the development of the Partnership for Critical Infrastructure Security, the maturing of Fusion Centers, and the Health Care CIKR sector.

## **Colors and Categories**

- There are effectively only 3 levels/colors in HSAS.
- The categorical nature of the system allows better planning and certainty about steps to be taken based on the threat level. Such a categorical level should be maintained.
- A categorical system such as the uniform military system (Alpha, Bravo, Charlie, Delta), Defcon and Force Protection Convention can be readily understood and drive:
  - uniform protection levels,
  - a common understanding of the system,
  - a quick, simple and understandable method of conveying to the public a heightened state of security and

- an increased readiness and preparedness posture to prevent an attack or mitigate its consequences.
- HSAS does not need to be five colors. Eliminating Blue and Green is recommended, especially if they are not likely to be used.
- Change the color-coded system to match the National Weather Service “Advisory,” “Watch,” and “Warning” levels.
- Alert flag may be sufficient. HSAS would be black or white if there is or is not an alert related to specific threat information.
- Establish a more severe top level. In some industries, red is a shut down, but could signify a severe threat or something having happened. Differentiate between these two.
- Include embedded in levels or as a level that private sector operators must respond.

### ***The Dynamics of Level Changes and Supplemental Information Provision***

- There is no description of an actual threat or recommended protective measures. Where details currently do exist, they are largely unavailable to the public or at least are less prominent than the color itself. Alternatively, the federal system is best served to provide information and allow more granular actionable response information to come from state, local, sector or individual firms.
- Include the specific federal government response in any change to the threat level.
- Changes in level should be more responsive to mitigation and barriers. This provides response to the efforts of private sector owners and operators as well as governmental entities to harden potential targets and make them more resilient. Thus about risk.
- Include an expiration of default time horizon for any changes, such as a reversion to the previous level after a certain number of days if not renewed by further information.
- Ability to distinguish between risks, such as airline vulnerabilities, and threats, such as the London plot. Managing of risks is on private sector’s shoulders unless a specific threat is levied. This eliminates many one-size fits all issues of responses to the general threat.

### ***System Uses and Tie-ins***

- It was both recommended and not recommended that there be alternative purposes to terrorism threat alerts, or an all-hazard approach.
- Allow an HSAS for the public and an enhanced version of the same system in a secure portal for a vetted community of both public and private sector entities.
- One way to implement the enhanced version is through a more granular internal system that eventually triggers changes in the public system.
- Make the targeted nature of the system both capable of being more “fine-tuned” and more targeted functionally and geographically. H1N1 in May 2009 provides an example of the issues associated with tying too closely to a system.

- Encourage smaller jurisdictions, sectors and private sector firms to devise their own systems that are tied into the federal system in tangible and quantifiable ways. This will produce better, more specific information and potentially increased resilience.
- Sector-specific and regional advisories are more useful than broad national ones.
- NLE 09 demonstrated the interconnectedness of the sector system. For instance, a change in the Oil and Gas sector forced a cascading change in the Chemical sector.
- Implications of changes are discretionary, leaving individuals to react. In highly regulated environments, there are many issues tied to HSAS as well as MARSEC.
- Maintaining a high alert level can be very expensive. Before government or private sector entities tie-in response, there must be sufficient assurance that levels will change within a reasonable time.
- It is likely that the use of HSAS within CIKR sectors will undergo further review following any changes to HSAS. They may be specified to meet the needs – especially the regulatory environments – of each sector.

**Alert system example: Multi-State Information Sharing and Analysis Center Cyber Alert Indicator**

The Multi-State Information Sharing and Analysis Center (MS-ISAC) has developed a Procedures and Protocols for Cyber Alert Indicator. The submitted document was adopted by the MS-ISAC October 31, 2006 and provides clear advice over a 5-level threat scheme in a simple seven-page document.

Associated with the indicator are the levels Green/Low, Blue/Guarded, Yellow/Elevated, Orange/High, Red/Severe. Examples, actions, and methods of notification are clearly and concisely stated for each level.

A simple formula is used to calculate the indicator level. This formula can easily be published with the changing threat level to better explain the cause for the change. The formula is as follows: *Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*. The indicator level is then computed from the Severity as follows:

<b>Alert Indicator Level</b>	<b>Severity</b>
<b>Green – Low</b>	-8 to -5
<b>Blue – Guarded</b>	-4 to -2
<b>Yellow – Elevated</b>	-1 to +2
<b>Orange – High</b>	+3 to +5
<b>Red – Severe</b>	+6 to +8

A secure portal allows each state in the MS-ISAC to set its own level and make it available to other ISACs, including brief narrative information regarding the reason for the current level, emergency contact information, the release of an advisory if appropriate citing details, and risks, and an integrated dashboard to view global cyber conditions at-a-glance.

The MS-ISAC's Procedures and Protocols for Cyber Alert Indicator are available from the Private Sector Office on request. A PowerPoint presentation on the secure portal is also available in the Private Sector Office.

**Alert system example: ASIS International Threat Advisory System Response Guidelines**

ASIS international has produced a guideline for private sector entity response at each of the current HSAS levels. This document does not address improvements or changes to the HSAS, but provides a comprehensive lens by which private sector thinking can be understood, including the many considerations for business continuity, personnel protection, and physical protection. The guideline aims to assist the reader to prepare plans, procedures and response strategies that may contribute to the mitigation of potential threats and risks. The guideline can be tailored to fit the needs of an organization and can be modified according to specific needs and circumstances.

ASIS primary concern is that there has been insufficient education regarding response to changes in the HSAS level. The system itself is not broken, but the vehicle by which it is communicated is not supported by an education program to turn the HSAS information into actionable results.

# **A Unified Emergency Scale from a Practitioner's View: A Public Warning System and Practitioner Notification System**

## **METHODOLOGY**

There are two groups of people who are to use the Unified Scale. First is to give information to the public. This needs to be both a warning system and an indicator of disaster related expectations. Second is to give information to practitioners. This is those in the emergency domain know what to expect and how to respond accordingly. A study was conducted on a group representing the public, but not the practitioner side.

### **Practitioner Population**

A group of 19 undergraduates majoring in Emergency Administration and Management in the United States were used. As part of the objectives of the course, the students were put into groups of 3 where each group represented a disaster type: tsunamis, earthquakes, volcanoes, floods, pandemics, wildfires, search and rescue, and hurricanes. These students had various levels of expertise and experience in the emergency domain. They all had participated in presenting their disaster group's scale, if a scale existed. If a scale did not exist, such as in the case of floods, volcanoes and wild fires, they offered ideas for scales and identified characteristics that were associated with their scales.

### **The Tasks**

There are two parts to this exercise. The first is to have a common scale identified by practitioners where there is a common lexicon for any given disaster situation. The second part is to elicit dimensions such that a more accurate reflection can be identified using Thurstonian derived scale.

### ***Scale Taxonomy***

In the first part, the students read the article published in a previous study on Unified Scales (Plotnick, Gomez, White and Turoff, 2007) for homework prior to the class two days prior. The day of the project, further explanations of the unified scale were discussed. The idea was presented verbally to the students discussion ensued until there was a full understanding of the task. As a group, and with much discussion between group members, the students were given 30 minutes to adopt their disaster to some sort of unified scale, be it the one given as an example in the previous work, or altered to fit a scale with such an idea.

### ***List Generation of Dimensions***

A week later, the students were given the task of eliciting their own disaster's dimensions of what was most important to society (or whatever the list was based on in Murray's original assignment).

These disaster groups then created an overall list which was ranked by all students independent one from the other. They voted on these items, could change their votes and discussion pursued in class as student saw their results. Their votes were anonymous and feedback was in the form of a bar chart using the course management system Moodle.

## RESULTS

### General Characteristics

#### *Colors*

Sixty-three percent of the submitted scales had both numbers and colors associated with their scales. All used numbers. Although the majority used colors, there was no consistency in any of the color usage. All used a predetermined scale using ranking systems either like a semantic differential or number to indicate low to high ends of the scale. Fifty percent of the scales used the word Level to indicate each step, while others used Tier or Code.

Table Unified Volcanoes	<b>Level 1</b>	<b>No risk</b>	<b>Dormant</b>	Suggested Scale for
	<b>Level 2</b>	<b>No immediate risk</b>	<b>Action may occur (Know what to do)</b>	
	<b>Level 3</b>	<b>Early warning plan</b>	<b>Start getting belongs together</b>	
	<b>Level 4</b>	<b>Plan comes into effect</b>	<b>Must leave</b>	
	<b>Level 5</b>	<b>Erupting</b>	<b>Should be gone</b>	

The Pandemic group presented their interpretation of how a Unified Scale could be utilized given this event using both numbers and colors.

We have based are unified scale based on Five tiers.

**Tier Zero-White color**

No disease is present in animals or humans

Response- no action taken

**Tier One**

A Disease found in animal, and also spreading to other animals.

Response- Vaccinations in animals to stop or slow the spread of the disease

**Tier Two**

Disease begins to spread to humans through contact with animals in a single country. Animals begin to die from the disease.

Response-Vaccine to humans, quarantine of infected humans and animals. Airplanes grounded in infected country.

**Tier Three**

Disease begins to spread through human to human contact across different countries. First human death occurs from the disease

Response-Borders shut down, Airplanes grounded internationally

**Tier Four**

Major disease outbreak, causing mass casualties worldwide.

Response-Martial Law in place, curfews enforced, Hazmat suiting must be worn, run to the hills, you are probably going to die, you are probably the only survivor

One group suggested also using +/- to better reflect the accuracy of information when levels are such that one instance of a measurement can take you from one level to another. This is in hopes that the public will make a more informed decision on preparatory or responsive events such as evacuations. In 2008 Hurricane Ike made landfall on Galveston Texas, a beach community. More than half of the residents stayed to ride out the storm. They were devastated and thousands had to be rescued from their homes due to the surge. Out of 5 categories, Ike was measured to be a 2 with wind speeds of 104 (look up) Had the wind speeds been one more mile per hour higher and Ike would have been a Category 3. Perhaps this extra bit of information could make a difference in public perception and then, in their response. Just as there is a big difference to a student if they receive a B+ versus a B-, there could also be delivered a message to the public during fuzzy times such as this.

## ***Numbers***

Numbers were used in every scale developed. All but one had the number *one* identified to be the lowest level, the safest level available. The other group started with *zero*. Five groups felt as though five distinct levels were all required for their disaster type while three other groups used six. The groups identified needing only 5 levels were: Search and Rescue, Hurricanes, Volcanoes and Pandemics. The disaster groups indicating that six levels were needed were: Tsunamis, Earthquakes and Tornadoes. This group each has at least one scale presently and all have many more levels than five. The group members indicated that having too many levels was too confusing, that greater distinction should be given with fewer levels.

## ***Dimensions***

<will fill in after exercise – no results yet>

## **THE UNIFIED SCALE**

### **Characteristics Required of a Unified Scale**

Colors can be misinterpreted and are used in a number of ways now by society. There is no common interpretation between colors and meaning. For example, in one scale submitted, Yellow was the lowest level where in another scale, it was the middle color, like in a stop sign. Colors can also be interpreted due to the nationality. One characteristic of a Unified Scale is that, when a person foreign to a geographic local, be it of the same country or different, they will know how to react due to the information given in the scale. A low level threat is a low level threat and is interpreted as such no matter the disaster where a high level means that it's time to take serious action.

All countries, all languages use a number system. One is one no matter the origin and can be interpreted as such as long as there is a common perception that one is the lowest level, perhaps zero would be better.

### **Disaster Types Altered to Fit Unified Scale**

#### ***Tsunamis***

There is no agreed upon scale for Tsunamis. Two scales presently exist and another is under development. This is probably in response to the Indian Ocean Tsunami of 2004. One reason for this could be that if disasters occur infrequently, the emphasis to develop a warning or response system is lower than a disaster which happens frequently in populated areas. For example, one of the best developed scales is the Hurricane Category system. Hurricanes hit the United States shores every year. The Tsunami scale is determined both numerically and by the size of the wave.

- |                                                            |
|------------------------------------------------------------|
| 1. <b>Very light.</b> Wave so weak. The people can't feel. |
|------------------------------------------------------------|

2. **Light.** Wave high about 1 meter. Can make a little damage.
3. **Rather strong.** Wave high about 2 meters. Can destruct house where close the beach.
4. **Strong.** Wave high about 4-6 meters. Can cause slightly more damage
5. **Very strong.** General flooding of the shore to some depth. Quay-walls and solid structures near the sea damaged. Light structures destroyed. Severe scouring of cultivated land and littering of the coast with floating items and sea animals. With the exception of big ships all other type of vessels carried inland or out to sea. Big bores in estuary rivers. Harbor works damaged. People drowned. Wave accompanied by strong roar.
6. **Disastrous.** Partial or complete destruction of manmade structures for some distance from the shore. Flooding of coasts to great depths. Big ships severely damaged. Trees uprooted or broken. Many casualties.

### ***Volcanoes***

There is no known scale for Volcanoes. However, a unified scale is offered. See Table x.x.

### ***Hurricanes***

Hurricanes happen frequently in developed areas. This is a system that has problems where fuzzy interpretations are caused due to the interval identifications. Improvements are proposed by adding an indicator of more than and less than. It is hoped that giving more information can better prepare both civilians and practitioners alike.

***Tornadoes***

Tornadoes occur frequently throughout the United States, both on their own accord and also as a secondary spawned by a Hurricane.

LEVEL 1	Incident
LEVEL 2	Minor Emergency
LEVEL 3	Major Emergency
LEVEL 4	Disaster
LEVEL 5	Extreme Event
LEVEL 6	Catastrophe

***Pandemics***

There is no known scale for Pandemics. However, a Unified Scale is offered indicating the need for one. See Table x.x.

***Wild Fires***

There is a warning system for Wild Fires which address the likelihood of a fire and it’s contain ability due to conditions such as humidity, drought, winds, etc. However, it’s believed that a Unified Scale could help both the public and private sector. The public would know if they should start looking for evacuation routes and emergency management would know how to address resource supply/demand requirements.

***Search and Rescue***

Search and Rescue has no scale. However, the practitioners felt that although a scale wouldn’t be required by the public sector, a scale could be greatly valued by practitioners.

Code 1	Light risk, no prominent factors requiring attention	Normal day
Code 2	Slight risk, factors are few but not uncommon	Holiday or other cause for grouping
Code 3	Medium risk, couple extra risk factors	Holiday with big grouping and an additional risk
Code 4	Moderate risk, multiple risk factors but no rescues to this point	big grouping, bad weather, and additional risks
Code 5	Heavy risk, multiple risk factors and there is a history or rescues	Foreigners bad weather, and many other risks

Hence, a Unified Scale could adapt its needs to the disaster type.

## *Earthquakes*

Earthquakes happen frequently, but the scale leaves an erroneous impression at best. It is complicated and is known by the public only after the fact. Destruction is correlated with the scale, but the practitioners felt that there were too many levels leaving too many interpretations due to the preciseness read from the seismograph.

Level 1	People cannot feel, stay safely
Level 2	Water shakes in the bottle. Tree swing.
Level 3	Paints, decorators fall from wall
Level 4	Houses shake strongly, people should leave them.
Level 5	Part of apartments or houses people got hurt or some of them are dead
Level 6	Every building falls down. People dead Casualties and fatalities seriously

## Response by Dr. Sutton of Natural Hazards Center

Comments on the Homeland Security Advisory System  
Provided to Ms Fran Townsend and Judge William Webster  
Co-Chairs, Task force on 60-Day Review Panel

Provided by: Dr. Jeannette Sutton  
Natural Hazards Center  
[suttonj@colorado.edu](mailto:suttonj@colorado.edu) 303-492-2150

These comments have been prepared by Jeannette Sutton, Ph.D., Research Associate, Natural Hazards Center, University of Colorado at Boulder, in response to a request for feedback about the effectiveness of the Homeland Security Advisory System. I am a disaster sociologist, specializing in warnings and communications to the public for extreme events. All comments and suggestions provided here draw upon knowledge obtained from empirical studies of human behavior in disaster.<sup>13</sup>

### 1. Is the HSAS effective in fulfilling its purposes as stated in HSPD-3?

The current HSAS is not an adequate system to alert or inform the public at risk about threats and protective actions. It does not provide effective warnings regarding the threat or risk that acts of terrorism will be committed on the homeland. It does not provide specific information or advice regarding appropriate measures and countermeasures that may be taken in response to the threat or risk. It does not create a common vocabulary, context, or structure for the discussion about threats and appropriate courses of action.

Specifically, the HSAS fails to link together disparate systems, to alert the public of impending threat, to provide adequate information of the impending threat or how to take protective actions. In addition, it fails to provide sufficient information to the public that will enable them to prepare for future events.

The unintended consequences of the HSAS include the following: the ongoing threat advisory levels (leaving the color code at an elevated level) has the potential to create a sense of complacency among members of the public; the lack of specific information about threats (location, hazard, protective actions to take) leaves members of the public in a state of confused apprehension; the lack of integration among the various warning systems implies a lack of collaboration or communication among systems and subsystems.

The fundamental goal of HSPD-3 is to increase what people know in order to impact their behavior. The way that the HSAS will become effective in fulfilling this purpose is to take into account the

---

<sup>13</sup> Additional information on human behavior in response to disaster warnings can be found here: <http://www.colorado.edu/hazards/publications/informer/infrmr2/pubhazbibann.pdf>. Additional information on behavior of building occupants in response to disaster warnings can be found here: <http://www.colorado.edu/hazards/library/BuildingsEvacBib2007.doc>.

corpus of knowledge developed by social scientists about people's behavioral responses to warnings and risk communication.

2. What changes, if any, would improve the current system?

A. In the most generous terms, the HSAS is a "Risk Classification System." It is not an alert system. It is not a warning system. It is not an advisory system. The function of the HSAS, as it currently stands, is to classify the risk to the American public and to link this to a set of color codes. An alert system will incorporate the risk classification and link it to specific mechanisms to get people's attention. A warning system will integrate risk classifications and alerts with messaging designed to get people to take protective action. These three elements build on each other; a warning must include an alert and an alert cannot be made until public officials determine that a specific threat has reached hazardous levels to warrant notifying the public. Underlying the entire system is public education designed to inform people of hazards and threats, the processes that will be used to notify them of a hazard, and the protective actions that they should take pre-event, during and event, and post-event.

To improve the current system, the first decision that must be made is whether or not the goal of HSPD-3 is to provide a risk classification system, an alert system, or a warning system. Once this decision has been made, a complete system can be designed taking into account each of these elements.

B. Develop a complete system. A complete alert and warning system takes into account all elements and subsystems and their functions and integrates these elements across all phases of disaster. Warning systems weave together disparate elements (technology, authorities, and the grass roots); disciplines (physical, social and behavioral sciences, and information and communication technology); specializations (inter-organizational relations, systems analysis, human factors, and social psychology); and societal divisions (varied government jurisdictions, public and private sectors, organizations, and the public). Included in these elements are subsystem actors (responsible for risk assessment, detection, management, and response), their relative functions (including but not limited to preparing, monitoring, detecting, warning and informing) and the linkages among subsystems across all phases of disaster.

Any effective warning system must take into account each of these components. The current HSAS, as viewed by members of the public, is simply a color-coded chart that gives non-specific information, linked to a non-specific location, and provides instruction to take non-specific protective actions. Furthermore, the HSAS appears to be suspended between the warning activities of threat detection and informing the public but does not provide adequate information on strategies to prepare for an impending event, nor how to effectively act/respond should an event occur.

C. Public education must become a part of the HSAS strategy.

Decades of empirical research on public preparedness leads disaster social scientists to claim that 'we know how to reach the public, how to teach the public, and how to motivate preparedness activity.' It is imperative that public education become an integral part of a warning system.

Warnings are effective insofar as members of the public are prepared to receive and act upon the messages provided. Preparing the public to respond to HSAS warning messages is vital to the success of future warning activities. This means that the public should have access to information about the type of threat, the nature of the threat, and how to take protective action in the event that a hazardous event occurs. Currently, information on various types of homeland security threats and response plans are ‘secured’ from public view. This makes the public less resilient to future hazards. In light of the HSPD-3 purpose of creating a common vocabulary for discussion about threats and appropriate courses of action, such information must be made available to those who are at risk. For instance, clear guidance on weapons of mass destruction and the various chemical, biological, radiological, and nuclear weapons that are of greatest concern should be provided. A common vocabulary can be developed around weapons which pose the greatest threat, chemical and radiological “dirty bombs,” or improvised explosive devices (IEDs) and should include their practical implications to society (rather than a focus on the scientific or legal definitions). Furthermore, this vocabulary should be linked to public education in order to ensure a state of readiness.

A “National Risk Register” similar to that found in the U.K.<sup>14</sup> could be developed and made available to the public online. Directly linked to the register could be information about practical steps to be taken ahead of time in preparation for an event. This would mirror the strategies taken for other types of risks within the natural environment such as earthquakes, tornadoes, hurricanes, and floods.

In addition making available relevant threat information, members of the public must be educated about the HSAS alert and warning system itself. This includes information regarding how they will receive an alert, from whom, where to go for additional warning information, specific protective actions that should be taken, and how they will be informed that the threat level has been decreased. For instance, the current Commercial Mobile Alert System, CMAS, is designed to send a 90-character message to all cell-phone carriers (by 2012) following the Common Alerting Protocol that includes a limited amount of information. While the CMAS alert will deliver alerts relative to specific geographical areas, the brevity of the alerting messages will require recipients to look elsewhere for more complete warning information. Without education on the meaning of the CMAS alert (which ideally will carry threat information included in the HSAS), members of the public will not have enough information to make informed decisions about the appropriate protective actions that they should be taking. This is likely to contribute to a great deal of apprehension and/or the sharing of misinformation as individuals use their personal social networks to make decisions about next steps to take.

D. Reconsider the various modes of information transmission to include multiple technology channels as well as social networks.

Warning systems for extreme events have long been designed in favor of a top-down, command and control model which relies heavily on experts for risk detection, decision making, and information dissemination. However, in the world of Web 2.0 communication modes and mechanisms are changing quickly. Members of the public are no longer reliant of information from public authorities, nor will they wait for official communications in times of need. Instead, they utilize

---

<sup>14</sup> [http://www.cabinetoffice.gov.uk/reports/national\\_risk\\_register.aspx](http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx)

social networks and networked communications to access information, to create and produce information, and to broadcast information to others.<sup>15</sup>

Informal communication activities (in contrast with official communications) are not new, however the channels through which they are communicated are evolving at a rapid pace. The internet provides new means for members of the public to share and confirm information with one another. It also provides a mechanism for public officials to connect with persons who more readily rely on online communications in contrast with major media for their preparedness and warning information.

Specific social media channels that can be utilized include wikis for collaborative information sharing about community risk, national risk, and protective actions; social networks such as Facebook or MySpace using widgets linked to key protective action information; microblogs, such as Twitter, which work as rapid or viral dissemination mechanisms for short text messages; and collaborative mapping for location-based information linked to key events or physical sites where help can be sought for evacuation, sheltering, decontamination, and other assistance. Videos or pictures demonstrating specific protective actions can be linked directly to alert and warning information via sites like YouTube or Flickr. Furthermore, educational campaigns can take advantage of multi-user online game technologies such Second Life.

While each of these online channels have drawbacks for government agencies (proprietary technologies, privacy issues, other legal restrictions and regulations), the benefits of their use and ability to reach members of the public in new and novel ways cannot be understated. Now that these technologies exist, members of the public will come to expect that local, state, and federal government will make use of them as effective means for communication.

#### E. Design effective warning messages.

The HSAS should take into account more than fifty years of empirical research on the design of effective warning messages. Disaster social scientists have conducted research that have taken into account and analyzed all of the known factors that affect one's behavior in response to a hazard or threat. The most salient issues which increase public responses to a warning message are the content of the warning message itself and its repetition.

An evidence based warning message is simply worded, precise and non-ambiguous, with no errors, presented with absolute certainty and is consistent. It provides information about what to do, when to do it, who should and shouldn't do it, the hazard and the consequences of the hazard, and who is giving the message. The message is confirmed repeatedly over multiple communication channels.

With the increase in type and reach of new communications channels, it is becoming more important for public authorities to utilize the channels in the delivery of warning messages. The delivery of consistent messages from key spokespersons can have greater reach and impact when utilizing new media online. When messages are ambiguous or delivered infrequently during a time in which threat levels are increased and individuals feel that their safety might be at risk, members of the public *will* seek out additional information through all available channels. Repetitive messaging

---

<sup>15</sup> For recent research highlighting the ways that members of the public access and create information using Web 2.0 technologies, see [www.jeanettesutton.com/papers\\_and\\_presentations](http://www.jeanettesutton.com/papers_and_presentations).

using social media has the potential to increase confidence in the message and direct individuals to take appropriate actions.

F. Conduct ongoing assessments of the effectiveness of alerts and social media.

Warning systems and messaging can be made more effective by building in feedback loops to evaluate the extent to which members of the public seek additional information and take protective action. Known as ‘milling’ this informal information seeking and sharing activity is a vital process in all warning activities. With the increase in Web 2.0 technologies, public officials can now observe milling online, evaluate the effect their messages are having, and tailor messages to produce the agency’s intended effect. Never before have governmental agencies had the ability to monitor public activities as they have today.

Real-time monitoring tools are being developed to help aggregate and assess public sentiment to messages. These same tools can identify key information hubs or connectors within social networks, providing insights into effective strategies to deliver messages that have an extended reach across the web. Furthermore, such monitoring activities can help to head off ‘bad public reputation’ issues by quickly identifying hot spots and hot issues that could direct the public away from protective action in times of crisis. Governmental agencies should utilize marketing strategies that are currently in place within the public sector to assess the reach that their messages are having and the responses that members of the public are taking.

3. For any improvements or changes proposed, what are the implications to public communications, security, costs, law/authorities, sociology, operations/governance, and other factors?

The changes proposed here are based upon decades of empirical research that has identified the critical elements of an effective warning system. The design of a complete warning system will require the integration of multiple sectors, systems, and subsystems. It will also require a change in information sharing and challenge the culture of secrecy that has developed in the post 9/11 era. In addition, specific suggestions related to the integration of new social media will require legal analysis relative to issues of privacy, proprietary software, copyright, and other restrictions or regulations. However, the governance issues are not new – the subsystem functions for a homeland security warning system mirror those for other hazards. What may differ for the HSAS is the set of specific partners who will function as actors within and across the alert and warning system.

These recommendations have focused almost entirely upon public responses to the HSAS. However, the most costly changes are likely to come within the private sector which has been given specific responsibilities in relation to each of the currently identified threat levels. Should the HSAS be changed, private sector entities will have to undergo significant planning for deployment, staffing, response, etc in order to comply with legal requirements.

# First Responder Stakeholder Outreach Summary Findings Report

## Overview and Sources

This report represents a consolidated overview of recommendations originating from the First Responder professional community, comprising law enforcement (LE), emergency management (EM), fire rescue (FR), and emergency medical services (EMS). While no work can comprehensively address the nuance-filled views, proposals and recommendations of such a talented and diverse professional community, this report presents those improvements to the Homeland Security Advisory System (HSAS) that received widespread community support, followed by novel proposals recommended for further consideration.

Input for this Summary Findings Report was obtained primarily through an intense roundtable discussion occurring on July 29, 2009. Leadership and Subject Matter Experts from more than a dozen major First Responder entities and professional associations participated in the two-hour session. Representing DHS were: Ed Delaney of I&A; Thomas Watson, DHS Honors Fellow; and Robert Patrick, Director of Medical First Responder Coordination, Office of Health Affairs. In addition to the conference call, the Office for State and Local Law Enforcement and the Office of Policy Development informed key stakeholders of the opportunity for free-form input into the HSAS review process, which has also been accounted for here.

## Universal Recommendations

The First Responder community uniformly identified the need for a Homeland Security Advisory System, and while the systems they envisioned differed significantly from the current form, all stakeholders advocated for a comprehensive state and local emphasis throughout the HSAS structure and operation. No stakeholders expressed feelings that the conceptual or practical need for a comprehensive threat advisory system was overstated or flawed. Most First Responders expressed feelings that the present system was grossly underpowered, and all stakeholders expressed the need for any HSAS to function as an “All-Threats, All-Hazards” system. Given the unique structure and broad mission of the Department, such an advisory system would be a natural utilization of existing DHS capabilities, and a force multiplier for other government resources. Additionally, stakeholders felt that the color-coded HSAS, while presently suffering from poor public imaging, is a familiar reference tool to security practitioners, the American population, and foreign entities.

Conceptually, some stakeholders believe the framework within HSPD-3 over-emphasizes the Federal government, limiting the system’s comprehensive, nation-wide functionality, especially when the federally-focused HSAS is used for implementing expensive readiness levels and response procedures for state and local governments, civic aid organizations, and ordinary citizens. This called into question if HSPD-3 itself required fundamental modification to properly define and authorize a HSAS given its present, ubiquitous use.

## Top Recommendations

The recommendations provided regarding the HSAS overwhelmingly called for greater specificity in the type and quality of information provided. All other recommendations largely pertained to the

operational and organizational components of the HSAS. Stakeholders felt that, in its current state, HSAS reports were largely useless, as they come unaccompanied by specific threat vectors, the geographic region targeted, recommended responses, or actionable intelligence with which to eliminate or avoid threats. To “reactive” entities – those primarily responsive to threats, such as fire services and the general public – unexplained shifts between advisory levels requiring no specific actions to avoid negative consequences can be met with apathy, undermining the legitimacy and efficacy of the entire system. Among other changes, stakeholders believe increased specificity in HSAS announcements and alerts would solve many of the system’s shortcomings.

## **Specificity**

The First Responder community proposed numerous changes to the HSAS critiquing the system’s specificity, or lack thereof. The authors have identified five recurring themes provided by First Responder stakeholders as essential components to be included in all HSAS alerts under a modified system: locality affected; sector targeted; threat vector(s); response actions; and, alert duration.

### ***Locality Affected***

All input provided regarding the HSAS called for additional information in the alerts; the most dominant theme was to have specific geographic information included with the advisory broadcast. Stakeholders generally expressed concern that a nationwide system provided little added-value for the county-level emergency manager, municipal central dispatch, patrol officers, or the local volunteer firefighter, each of which must respond to tactical, point-specific incidents.

For instance, intelligence indicating a terrorist threat in New York City should not elevate the threat level in Butte, Montana. Similarly, a Southern California brushfire, no matter how large, should not elevate the threat code for Miami-Dade County. Under the current system, should the alert level be raised, there is no differentiation between localities, which may be separated by hundreds of miles. A nation-wide threat elevation results in the disruption of security and health service delivery, and in the increased use of limited state and local resources within areas facing minimal risk.

First Responders desired the greatest granularity and scalability possible in any revised HSAS; several expressing an interest in having a new HSAS capable of advisory alerts and situational awareness specific to the city block and neighborhood-level. Such a system could “piggy-back” on existing open and closed-source real-time information networks, such as severe weather alerts, traffic monitoring, computer-aided dispatchers, and municipal watch systems (e.g. – CCTV, gunshot location).

### ***Sector Targeted***

Most First Responders had positive views towards the existing sector-specific threat categories. Stakeholders expressed that all DHS alerts should explicitly list the sectors at risk – financial, airline, power, etc. – in order to enable improved operational planning and threat response.

### ***Threat Vector(s)***

Just as the location and sector of a threat have been listed as imperative qualities in a revised HSAS, Responders were emphatic that the threat vector(s) be disclosed as much as possible. For First Responders, contingency planning for “lone gunman,” coordinated Mumbai-style assault, VB-IED, hurricane, pandemic, and a nuclear reactor containment failure are vastly different to each other and

are not interchangeable. Many of these plans require significant preparation and equipment staging to execute properly.

### ***Response Actions***

The second most common recommendation relating to specificity was that the HSAS is not linked to a formal response framework for non-federal entities. An elevation in the threat level should be accompanied with a breakdown of what the Federal government is doing to respond, as well as recommended or required response actions for First Responders, local government, targeted sector entities, and, if needed, the general population, including special needs/ at-risk groups. Response actions should be designated as “recommended” or “required” according to the nature, saliency and proximity of the particular threat.

### ***Alert Duration***

The final major component to accompany an updated HSAS would be a specific window in which the alert and/or elevated threat would be in effect. The most notable point of concern among the First Responder professional community was the exceedingly long time that the airline sector has been at “orange” or “High alert.” It was strongly recommended that alerts which raise the threat condition above the lowest, baseline state should be effective only to a specific date, upon which time the warning is either reissued to extend the alert status or the threat condition is reduced to the lowest level allowed, given any other active advisory alerts. Not only would this provide significant cost savings for government entities and the private sector, but it could increase the system’s legitimacy to the public, showing that homeland security threats can and do, develop, peak, diminish and reemerge over time.

### **Fusion Center(ed)**

The First Responder community strongly supported linking the HSAS to DHS’ fusion center network. This proposal was promoted by each participating community (LE, EM, FR, EMS) reporting that fusion centers provide the necessary functions of disseminating information and coordinating response without the need for any new organizational structures or programs. It should be noted that many First Responders are already linked directly to one of the 70-odd fusion centers across the nation. This connectivity provides access and visibility to their own state and local operational counterparts, executive leadership, federal entities and, most importantly, authoritative non-media information sources. Stakeholders noted two key advantages of operating the HSAS through the fusion centers; it allows the secure distribution of classified material, and it can provide a single-source of novel, non-media information.

Fusion centers already operate in a manner that allow state and local law enforcement, fire, emergency medical, and disaster management teams to collaborate with each other and with federal law enforcement, military, and intelligence entities. Fusion centers have the procedures and protocols for protecting and disseminating sensitive information to those needing it, such as law enforcement, while coordinating emergency response efforts (e.g. - fire, EMS) across jurisdictional and bureaucratic lines without disclosing protected information. HSAS alerts channeled through fusion centers could contain significantly more need-to-know information for locals, especially law enforcement, to craft prevention and response strategies while preventing the release of classified intelligence. From a Departmental standpoint, having the HSAS advisory network based out of

fusion centers can mature the fusion network, encouraging organizational and operational development with robust, value-added tools that build on local abilities and resources.

In providing intelligence and secure information to First Responders, the fusion centers would act as official, authoritative nationwide information and communications networks. With 24-hour, real-time news available, DHS must provide situational awareness not provided by standard media outlets in order to remain a prominent and salient information resource in times of crisis. The Department's fusion centers can leverage the significant information and analytic resources of the full federal government – including DoJ/ FBI, DoD/DIA, NOAA – to validate the underlying assumptions driving decisions of the state and local security partners, while facilitating a coordinated response between public sector, non-governmental organizations and local, state and federal entities, regardless of threat or challenge. This would require a consolidation or housing of existing threat identification and notification systems within the fusion center (including those that are weather-based), but doing so would eliminate confusion and source validity regarding potential or actual disruptive events – the fusion center becomes the single-source distribution point for all homeland security-based information and messaging.

### **A Two-Way Exchange**

Given an “All-Threats, All-Hazards” mandate, it is entirely conceivable that a local fusion center may find a pressing need to alert the federal government of a nation-wide homeland security threat, manmade or natural. The first responder community felt that a crucial component lacking in the current HSAS is a method by which state and local government agencies – or even citizens – can raise or lower the HSAS Threat Assessment level. If the HSAS were redesigned as a comprehensive advisory system to be used primarily by state and local entities, the ability to autonomously increase local alert levels could be particularly useful to warn citizens and business of small-scale incidents and to coordinate regional response efforts. Alternatively, in some situations it may be equally beneficial for trained “boots on the ground” to recommend an early reduction in the alert level should a threat not materialize or prove less severe than expected.

### **Other Recommendations**

Among the most controversial recommendations discussed during the roundtable and provided through email were those of HSAS funding and public messaging. Both issues should deserve considerable and in-depth consideration in the larger HSAS Review process.

### **Funding for High Threat Levels**

Across all disciplines, First Responders seemed evenly divided as to whether or not the HSAS, particularly its highest awareness levels, should have funding allowances linked to them. Proponents of such a system noted that the funding assured state and local entity involvement and adherence to the HSAS. Opponents remarked that having funding tied to alert levels creates an economic and political incentive for prolonged threats, leading to broadened allowable UASI grant spending at the expense of planned, strategic homeland security projects. One possible solution under an improved HSAS would have funding based on response actions mandated for a specific threat, not the level of threat itself. In many cases, an alert should require only increased situational awareness, not a tangible increase in resource use. Should the alert go up to a level where funds can be used, it should be for very limited duration to neutralize an identified threat or respond to an event.

## **Public Messaging**

Most of the First Responder stakeholders seriously questioned the value of a publicly disclosed HSAS. Many noted that the current HSAS serves little function to alter the behavior of the general population. The perception among First Responders is that the public has no real involvement in eliminating or neutralizing homeland security threats. Additionally, any information or messaging the public receives can, and usually does, come from broadcast media and official public messaging. First Responder stakeholders felt that elevating the threat level has no meaning to the public unless individuals are compelled to alter behavior to avoid negative consequences. If the recommended specificity points (locality, sector, threat vectors, response actions, threat duration) are included for the general public, this perception could quickly change.

Some First Responders recommended the HSAS have multiple layers of information, such as discreet components for open or public messaging, sector-specific partners (private sector/ CIKR), first responders, law enforcement, and classified intelligence. Under such a system, the public portion of the HSAS would be a relatively minor section of the overall framework, and could offer general situational awareness information with an emphasis on response and prevention. Such an approach could capitalize on other Departmental programs and missions, and would reinforce a fusion center based approach for the HSAS.

# Pennsylvania Emergency Management Agency Suggestions

## Review and Suggestions for the Homeland Security Advisory System

August 7, 2009

Thank you for the opportunity to provide comments and suggestions on the Homeland Security Advisory System (HSAS). The HSAS has been a problematic and difficult program for states to both respond to and articulate to the public since its inception in 2001 and we look forward to a thoughtful and deliberate review of the system. In general, we view the system with two distinct, but currently connected purposes:

- to inform the public of threats; and
- to inform public officials and the first responder community associated with critical infrastructure/key resources (CIKR) of potential threats to their assets.

The two purposes should not be combined in a one size fits all system and the attempt to do so has left both audiences without actionable information and a sense of complacency. The HSAS has therefore lost some credibility.

Generally the HSAS:

- is too vague to provide any helpful information to the public;
- fails to convey the specific threat and protective actions for the targeted population;
- remains at a heightened state, since its inception, rendering the “yellow status” useless and the new baseline state, which may actually cause the public to become less vigilant and more apathetic and complacent;
- is subject to political manipulation; and
- inadvertently promotes confusion, apathy, and fear consumption.

Raising and lowering the national threat level makes a significant statement to the public regarding the government’s assessment of public safety. Raising the level has direct implications:

- costly local government and private sector protective measures for generalized threats;
- changes in personal behavior;
- personal safety fears;
- changes in travel and spending patterns; and
- corresponding effect on the nation’s economy (nationally, regionally, locally and/or sector-specific).

Integrated warning systems should have a standardized, repeatable process with defined criteria for both issuing and terminating public warnings. The more scientifically valid, reliable and effective the information that is shared, the more credibility the system will have.

An integrated warning system should include:

- creation of specific threat warning;
- designation of the specific sector under threat;
- dissemination of the warning; and
- public education about the threat and protective action steps.

The messages should be:

- clear and understandable;
- accurate, frequent, credible;
- specific to the danger and likely effect of the hazard on a specific location or sector - not nationwide; and
- used to provide information to minimize vulnerability.

## **Recommendation**

Establish and communicate a baseline of everyday protective measures that the general public should take now to prepare themselves for all hazards incidents. This would include the steps recommended currently for threat levels Green, Blue and Yellow and the general [ready.gov](https://www.ready.gov) recommendations.

Utilize two processes to communicate threat information:

- a two-tiered, simple system for the general public about situations we are able to openly discuss (Section 201 (d) (7) (a) of the Homeland Security Act of 2002); and
- direct communication with local governments and the private sector with specific information and protective actions they should take for situations that do not allow for public disclosure of information (Section 201 (d) (7) (b) of the Homeland Security Act of 2002).

The new warning system for the general public should eliminate the confusing, vague, multi-tiered, color-coded HSAS. Implement a two- tiered system, similar to the national weather service watch/warning system. Alerts should be issued in brief terms, using simple plain English, providing specific information on the potential threat and protective actions required. The alert should be targeted to the specific geographic region or CI/KR sector affected. The alert should include an expiration time. If the threat is too vague or too sensitive to localize to a specific geographic area or sector and no protective measures are recommended, beyond the everyday measures discussed above, serious consideration should be given to not releasing the information. Providing a threat warning and then telling people to go on about their lives, without any recommended actions to take, sends a very confusing message. Clear protocols should be put into place that are easily understandable at all levels of government and with the general public about how and when to issue the alert. Dissemination of this alert or warning should not be used to convey information to law enforcement, government officials or CI/KR sectors. They should be notified using the system described below.

The HSAS was created prior to the implementation of information and analysis fusion centers within the states and the Federal government. These centers and networks provide the ideal

environment for sharing specific and actionable threat information to law enforcement officials, government officials and representatives of the affected CI/KR sectors. There is no need to utilize a general, public warning system for these entities. These stakeholders require specific information in order to protect assets, mitigate effects and potentially prevent the threat from occurring. These entities are not the end user of a national threat system and trying to include them will water down the message given to them and will confuse the message to the public.

Thank you for allowing us the opportunity to comment of the HSAS.

#### References:

Aguirre, Benigno E. "Homeland Security Warnings: Lessons Learned and Unlearned". Disaster Research Center, University of Delaware

Congressional Hearing. "The Homeland Security Advisory System, Hearing before the Select Committee on Homeland Security, House of Representatives." February 4, 2004. Serial No. 108-35.

Paul, John and Sangyoub Park, Washburn University. "With the Best of Intentions: The Color Coded Homeland Security Advisory System and the Law of Unintended Consequences". *Research and Practice in Social Sciences*, Volume 4, No.2 (February 2009) 1-13

Shapiro, Jacob N. and Dara Kay Cohen. "Lessons from the Failed Homeland Security Advisory System." *International Security*, Vol. 32, No. 2 (Fall 2007), 121-154.